Status:	**Active Policy**
Effective Date:	September 24, 2006 through September 23, 2008
Revised Date:	N/A
Approved By:	J. Stephen Fletcher, CIO
Authority:	*UCA §63F-1-103; UCA §63F-1-206; Governor's Executive Order: Directing the Chief Information Officer to Develop and Implement Policy Promoting Security of State Information and Information Systems*

1250.1 PURPOSE

The purpose of this policy is to ensure that all computer security related incidents are reported to a coordinating group to assure incidents are handled appropriately and information is gathered on all security incidents.

1250.1.1 Background

Reporting incidents to a central coordinating group promotes collaboration and information sharing with other agencies that may be experiencing the same problems. Some of the benefits this provides include the following:

- The ability to coordinate activities among *state entities* experiencing similar incidents to help identify and resolve the problem more quickly than if done separately.
- The ability to coordinate similar *state entities* that may be pursuing legal actions against the intruder.
- The ability to warn and share preventative information to help other *state entities* protect themselves from similar attacks.
- The ability to collect statewide information on the types of vulnerabilities that are being exploited, frequency of attacks and cost of recovering from an attack.

1250.1.2 Scope

This policy applies to all employees and contractors within the Department of Technology Services (DTS).

1250.1.3 Exceptions

Agencies excluded under the provisions of *§63F-1-102 (7) et seq.,* are not included under the provisions of this policy.

1250.2 DEFINITIONS

Computer Security Incident
Computer Security Incidents are defined as an unexpected, unplanned event that could

have a negative impact on IT resources, or disruption in IT services, and requires immediate action to prevent further negative impacts or loss of service, and/or violates security policies.

1250.3 POLICY

1250.3.1 It is the responsibility of all DTS employees and contractors to report suspected computer incidents as quickly as possible. The goal, regardless of the incident, is the protection of assets, containment of damage, and restoration of service.

1250.3.2 The DTS Enterprise Information Security Office shall establish and enforce a procedure for reporting computer security related incidents.

1250.3.3 All security incidents, including possible security incidents, shall be reported to the Enterprise Information Security Office (EISO) following the established Computer Security Incidents Reporting Procedure.

1250.3.4 The IT Director of each DTS supported agency shall assign an individual to be a member of the State of Utah Computer Information Security Response Team. (UT.CSIRT). The IT Director or designee is responsible to ensure that the contact information for the assigned individual remains current and appraise UT.CSIRT of any changes.

1250.3.5 Information regarding specific security measures or security-related incidents will not be publicly disclosed by any DTS employee or contractor unless such action is approved by the DTS Enterprise Information Security Office or the CIO.

1250.4 POLICY COMPLIANCE

1250.4.1 Employees found to have intentionally violated a provision of this policy may be subject to disciplinary action.

1250.4.2 If an employee's violation of this policy results in either personal gain to that employee, or personal harm or loss to a client, the State, or another employee, disciplinary action is generally warranted. If disciplinary action is not taken, the employee's Supervisor shall document the violation, the gravity of the violation, and the extent of the resulting gain or losses, and the reasons why disciplinary action was not warranted in the particular situation.

DOCUMENT HISTORY

Originator:	Michael Casey, Chief Information Security Officer
Next Review:	August 10, 2009
Reviewed Date:	N/A
Reviewed By:	N/A